

# Improved Perfect Space-Time Block Codes

K. Pavan Srinath and B. Sundar Rajan, *Senior Member, IEEE*

Dept of ECE, The Indian Institute of Science,

Bangalore-560012, India

Email: {pavan,bsrajan}@ece.iisc.ernet.in

**Abstract**—The perfect space-time block codes (STBCs) are based on four design criteria - full-rateness, non-vanishing determinant, cubic shaping and uniform average transmitted energy per antenna per time slot. Cubic shaping and transmission at uniform average energy per antenna per time slot are important from the perspective of energy efficiency of STBCs. The shaping criterion demands that the *generator matrix* of the lattice from which each layer of the perfect STBC is carved be unitary. In this paper, it is shown that unitariness is not a necessary requirement for energy efficiency in the context of space-time coding with finite input constellations, and an alternative criterion is provided that enables one to obtain full-rate (rate of  $n_t$  complex symbols per channel use for an  $n_t$  transmit antenna system) STBCs with larger *normalized minimum determinants* than the perfect STBCs. Further, two such STBCs, one each for 4 and 6 transmit antennas, are presented and they are shown to have larger normalized minimum determinants than the comparable perfect STBCs which hitherto had the best known normalized minimum determinants.

**Index Terms**—Cyclic division algebra, Galois group, MIMO systems, non-vanishing determinant, shaping criterion, space-time block codes.

## I. INTRODUCTION AND BACKGROUND

The perfect STBCs for multiple input, multiple output antenna (MIMO) systems were introduced in the landmark paper [1] for 2, 3, 4 and 6 transmit antennas. These were designed to meet four important criteria, namely

- 1) full-rateness of space-time block codes (STBCs).
- 2) non-vanishing determinant (NVD) (see Definition 3).
- 3) constellation cubic shaping (see subsection II-C).
- 4) uniform average transmitted energy per antenna per time slot.

The first and the second criteria were shown to be sufficient for diversity-multiplexing gain (DMT)-optimality and approximate universality [2]. The third and the fourth criteria were framed from the perspective of energy efficiency and hence coding gain. Later, perfect STBCs were constructed for arbitrary number of transmit antennas in [3]. The perfect STBCs in general have among the largest known normalized minimum determinants (see Definition 1) among existing STBCs in their comparable class and in particular, the perfect STBCs of [1] have the largest known normalized minimum determinants for 2, 3, 4 and 6 transmit antennas. However, we note that the cubic shaping criterion, which demands that the generator matrix of each layer [1] of the codeword matrices of perfect STBCs be unitary, is not a necessary criterion (although sufficient) for energy efficiency in the context of space-time coding with discrete input constellations. We propose

an alternative criterion that preserves energy-efficiency and enables one to obtain STBCs with larger normalized minimum determinants than the perfect STBCs of [1] while meeting the other three design criteria. We then show the existence of one such STBC in literature for 4 transmit antennas which has the best normalized minimum determinant. This STBC was first proposed in [4] but its superior coding gain was not identified. We then present a new STBC for 6 transmit antennas which, to the best of our knowledge, has the largest normalized minimum determinant for 6 transmit antennas. We call these STBCs improved perfect STBCs (see Definition 5 in Section III).

## A. Contributions and paper organization

The contributions of this paper may be summarized as follows.

- 1) We propose a modified shaping criterion that enables one to obtain rate- $n_t$  STBCs with larger coding gains than the perfect STBCs while retaining all the other desirable properties of the perfect STBCs.
- 2) For 4 and 6 transmit antennas, we present such STBCs which have a larger normalized minimum determinant than the comparable perfect STBCs.

The paper is organized as follows. In Section II, we give the system model, relevant definitions and a brief overview of perfect STBCs. Section III presents the modified shaping criteria while the improved perfect STBCs for 4 and 6 transmit antennas are presented in Sections IV and V, respectively. Appendix I provides some basic definitions and results in number theory which are used in this paper.

## Notations

Throughout the paper, the following notations are used.

- Bold, lowercase letters denote vectors, and bold, upper-case letters denote matrices.
- $\mathbf{X}^H$ ,  $\mathbf{X}^T$ ,  $\det(\mathbf{X})$ ,  $\text{tr}(\mathbf{X})$  and  $\|\mathbf{X}\|$  denote the Hermitian, the transpose, the determinant, the trace and the Frobenius norm of  $\mathbf{X}$ , respectively.
- $|\mathcal{S}|$  denotes the cardinality of the set  $\mathcal{S}$  and for the set  $\mathcal{T} \subset \mathcal{S}$ ,  $\mathcal{S} \setminus \mathcal{T}$  denotes the set of elements of  $\mathcal{S}$  not in  $\mathcal{T}$ .
- $\mathbf{I}$  and  $\mathbf{O}$  denote the identity matrix and the null matrix of appropriate dimensions.
- $\mathbb{E}(X)$  denotes the expectation of the random variable  $X$ .
- $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{Q}$  denote the field of real, complex and rational numbers, respectively.  $\mathbb{Z}$  denotes the ring of rational integers.

- Unless used as a subscript or a superscript,  $i$  denotes  $\sqrt{-1}$  and  $\omega$  denotes the primitive third root of unity.
- For fields  $\mathbb{K}$  and  $\mathbb{F}$ ,  $\mathbb{K}/\mathbb{F}$  denotes that  $\mathbb{K}$  is an extension of  $\mathbb{F}$  and  $[\mathbb{K} : \mathbb{F}] = m$  indicates that  $\mathbb{K}$  is a finite extension of  $\mathbb{F}$  of degree  $m$ .
- $\text{Gal}(\mathbb{K}/\mathbb{F})$  denotes the Galois group of  $\mathbb{K}/\mathbb{F}$ , i.e., the group of  $\mathbb{F}$ -linear automorphisms of  $\mathbb{K}$ .
- For an element  $a$  of a ring  $\mathcal{R}$ ,  $a\mathcal{R}$  denotes the ideal of  $\mathcal{R}$  generated by  $a$ .

## II. SYSTEM MODEL AND DEFINITIONS

We consider an  $n_t$  transmit antenna,  $n_r$  receive antenna MIMO system ( $n_t \times n_r$  system) with perfect channel-state information available at the receiver (CSIR) alone. The channel is assumed to be quasi-static with Rayleigh fading. The system model is

$$\mathbf{Y} = \rho \mathbf{H} \mathbf{S} + \mathbf{N}, \quad (1)$$

where  $\mathbf{Y} \in \mathbb{C}^{n_r \times T}$  is the received signal matrix,  $\mathbf{S} \in \mathbb{C}^{n_t \times T}$  is the codeword matrix that is transmitted over a block of  $T$  channel uses,  $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$  and  $\mathbf{N} \in \mathbb{C}^{n_r \times T}$  are respectively the channel matrix and the noise matrix with entries independently and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with zero mean and unit variance. The average signal-to-noise ratio (SNR) at each receive antenna is denoted by  $\rho$ . It follows that

$$\mathbb{E}(\|\mathbf{S}\|^2) = T. \quad (2)$$

A space-time block code (STBC)  $\mathcal{S}$  of block-length  $T$  for an  $n_t$  transmit antenna MIMO system is a finite set of complex matrices of size  $n_t \times T$ . An STBC transmitting  $k$  independent complex information symbols in  $T$  channel uses is said to have a rate of  $k/T$  complex symbols per channel use. Throughout the paper, we consider linear STBCs [5] whose codeword matrices are of the form  $\mathbf{S} = \sum_{i=1}^k s_i \mathbf{A}_i$  where the  $k$  independent information symbols  $s_i$  take values from a complex constellation  $\mathcal{A}_q$  which is QAM or HEX, and  $\mathbf{A}_i$ ,  $i = 1, \dots, k$ , are the complex weight matrices of the STBC. An  $M$ -PAM,  $M$ -QAM and  $M$ -HEX with  $M = 2^a$ ,  $a$  is even and positive, are respectively given as

$$\begin{aligned} M\text{-PAM} &= \{-M+1, -M+3, -M+5, \dots, M-1\}, \\ M\text{-QAM} &= \{a + ib, a, b \in \sqrt{M}\text{-PAM}\}, \\ M\text{-HEX} &= \{a + \omega b, a, b \in \sqrt{M}\text{-PAM}\}. \end{aligned}$$

Among STBCs transmitting at the same rate in bits per channel use, the metric for comparison that decides their error performance is the normalized minimum determinant which is defined as follows.

**Definition 1: (Normalized minimum determinant)** For an STBC  $\mathcal{S}$  whose codeword matrices satisfy (2), the normalized minimum determinant  $\delta_{\min}(\mathcal{S})$  is defined as

$$\delta_{\min}(\mathcal{S}) = \min_{\mathbf{s}_i, \mathbf{s}_j \in \mathcal{S}, i \neq j} \left\{ |\det(\mathbf{S}_i - \mathbf{S}_j)|^2 \right\}. \quad (4)$$

For full-diversity STBCs,  $\delta_{\min}(\mathcal{S})$  defines the coding gain [6]. Between two competing STBCs, the one with the larger

normalized minimum determinant is expected to have a better error performance.

**Definition 2: (STBC-scheme [7])** An STBC-scheme  $\mathcal{S}_{sch}$  is defined as a family of STBCs indexed by  $\rho$ , each STBC of block length  $T$  so that  $\mathcal{S}_{sch} = \{\mathcal{S}(\rho)\}$ , where the STBC  $\mathcal{S}(\rho)$  corresponds to a signal-to-noise ratio of  $\rho$  at each receive antenna.

**Definition 3: (Non-vanishing determinant [8])** A linear STBC-scheme  $\mathcal{S}_{sch} = \{\mathcal{S}(\rho)\}$ , all of whose STBCs  $\mathcal{S}(\rho)$  are defined by weight matrices  $\{\mathbf{A}_i, i = 1, \dots, k\}$  and employ complex constellations (QAM or HEX) that are finite subsets of an infinite complex lattice  $\mathcal{A}_L$  ( $\mathbb{Z}[i]$  or  $\mathbb{Z}[\omega]$ ), is said to have the non-vanishing determinant (NVD) property if  $\mathcal{S}_{\infty} \triangleq \left\{ \sum_{i=1}^k s_i \mathbf{A}_i \mid s_i \in \mathcal{A}_L \right\}$  is such that

$$\min_{\mathbf{s} \in \mathcal{S}_{\infty}, \mathbf{s} \neq \mathbf{0}} \{ |\det(\mathbf{S})|^2 \} = c > 0$$

for some strictly positive constant  $c$ .

**Definition 4: (Generator matrix of an STBC)** For a linear STBC that is given by  $\mathcal{S} = \left\{ \sum_{i=1}^k s_i \mathbf{A}_i \right\}$ , the generator matrix  $\mathbf{G} \in \mathbb{C}^{n_t \times k}$  is defined as [5]

$$\mathbf{G} = [\text{vec}(\mathbf{A}_1) \text{vec}(\mathbf{A}_2) \dots \text{vec}(\mathbf{A}_k)]$$

where the operation  $\text{vec}(\mathbf{A})$  denotes the vector obtained by stacking the columns of  $\mathbf{A}$  one below the other.

### A. Cyclic Division Algebras

A cyclic division algebra (CDA)  $\mathcal{A}$  of a degree  $n$  over a number field  $\mathbb{F}$  is a vector space over  $\mathbb{F}$  of dimension  $n^2$ . The center of  $\mathcal{A}$  is  $\mathbb{F}$  and there exists a maximal subfield  $\mathbb{K}$  of  $\mathcal{A}$  such that  $\mathbb{K}$  is a Galois extension of degree  $n$  over  $\mathbb{F}$  with a cyclic Galois group generated by  $\tau$ .  $\mathcal{A}$  is a right vector space over  $\mathbb{K}$  and can be expressed as

$$\mathcal{A} = \mathbb{K} \oplus \mathbf{i}\mathbb{K} \oplus \mathbf{i}^2\mathbb{K} \oplus \dots \oplus \mathbf{i}^{n-1}\mathbb{K},$$

where  $\mathbf{a}\mathbf{i} = \mathbf{i}\tau(a)$ ,  $\forall a \in \mathbb{K}$ ,  $\mathbf{i}^n = \gamma$ , for some  $\gamma \in \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$  such that the norm  $N_{\mathbb{K}/\mathbb{F}}(a) = \prod_{i=0}^{n-1} \tau^i(a)$  of any element  $a \in \mathbb{K}$  satisfies

$$N_{\mathbb{K}/\mathbb{F}}(a) \neq \gamma^t, \quad t = 1, \dots, n-1. \quad (5)$$

The CDA  $\mathcal{A}$  is denoted by  $(\mathbb{K}/\mathbb{F}, \tau, \gamma)$ .  $\mathcal{A}$  has a matrix representation and in particular, an element  $a_0 + \mathbf{i}a_1 + \dots + \mathbf{i}^{n-1}a_{n-1}$  of  $\mathcal{A}$ , where  $a_i \in \mathbb{K}$ , has the representation shown in (3) at the top of the next page. In addition, every nonzero matrix of the form shown in (3) is invertible and its determinant lies in  $\mathbb{F}^\times$  [10], i.e.,

$$\det(\mathbf{F}) \in \mathbb{F}^\times, \quad \mathbf{F} \neq \mathbf{O}. \quad (6)$$

For more on CDAs, one can refer to [10], [11] and references therein.

### B. STBCs from CDA

For the purpose of space-time coding, the signal constellation is generally  $M$ -QAM or  $M$ -HEX which are finite subsets of  $\mathbb{Z}[i]$  and  $\mathbb{Z}[\omega]$ , respectively. So,  $\mathbb{F}$  is naturally chosen to be  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\omega)$  for which the ring of integers

$$\mathbf{F} = \begin{bmatrix} a_0 & \gamma\tau(a_{n-1}) & \gamma\tau^2(a_{n-2}) & \cdots & \gamma\tau^{n-1}(a_1) \\ a_1 & \tau(a_0) & \gamma\tau^2(a_{n-1}) & \cdots & \gamma\tau^{n-1}(a_2) \\ a_2 & \tau(a_1) & \tau^2(a_0) & \cdots & \gamma\tau^{n-1}(a_3) \\ a_3 & \tau(a_2) & \tau^2(a_1) & \cdots & \gamma\tau^{n-1}(a_4) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n-1} & \tau(a_{n-2}) & \tau^2(a_{n-3}) & \cdots & \tau^{n-1}(a_0) \end{bmatrix}. \quad (3)$$

are respectively  $\mathbb{Z}[i]$  and  $\mathbb{Z}[\omega]$ , and a CDA  $\mathcal{A}$  of degree  $n_t$  over  $\mathbb{F}$  is constructed. We denote the ring of integers of  $\mathbb{F}$  and  $\mathbb{K}$  by  $\mathcal{O}_{\mathbb{F}}$  and  $\mathcal{O}_{\mathbb{K}}$ , respectively. The codeword matrices of the STBC obtained from the CDA  $\mathcal{A}$  have the structure shown in (3) with  $a_i$ ,  $i = 1, 2, \dots, n_t$ , expressed as linear combinations of elements of some chosen  $\mathbb{F}$ -basis over  $\mathcal{O}_{\mathbb{F}}$ , and hence STBCs from CDAs encode  $n_t^2$  complex information symbols in  $n_t$  channel uses. An STBC  $\mathcal{S}$  that is obtained from CDA is expressible (prior to SNR normalization) as  $\mathcal{S} = \left\{ \sum_{i=1}^{n_t} s_i \mathbf{A}_i, s_i \in \mathcal{A}_q \right\}$  where  $\mathcal{A}_q$  is either QAM or HEX, and  $\mathbf{A}_i$ ,  $1, \dots, n_t$ , are the complex weight matrices. The following proposition relates the choice of  $\mathbb{F}$ -basis to the NVD property of STBC-schemes that are based on STBCs from CDA.

*Proposition 1:* An STBC-scheme that is based on STBCs from CDA has a non-vanishing determinant if all the elements of the  $\mathbb{F}$ -basis belong to  $\mathcal{O}_{\mathbb{K}}$ .

*Proof:* Consider the STBC-scheme  $\mathcal{S}_{sch} = \{\mathcal{S}(\rho)\}$ , where all the  $\mathcal{S}(\rho)$  are obtained from the same CDA and given by  $\mathcal{S}(\rho) = \left\{ \beta \sum_{i=1}^{n_t} s_i \mathbf{A}_i, s_i \in \mathcal{A}_q(\rho) \right\}$ , where  $\mathcal{A}_q(\rho)$  is the regular QAM or HEX constellation whose size is dependent on  $\rho$  so that the required multiplexing gain is achieved (see [2] for details), and  $\beta$  is the normalizing scalar that ensures that the average energy at each receive antenna is  $\rho$ . From Definition 3,  $\mathcal{S}_{sch}$  has the NVD property if  $\mathcal{S}_{\infty} = \left\{ \sum_{i=1}^{n_t} s_i \mathbf{A}_i, s_i \in \mathcal{O}_{\mathbb{F}} \right\}$  ( $\mathcal{O}_{\mathbb{F}}$  is either  $\mathbb{Z}[i]$  or  $\mathbb{Z}[\omega]$ ) is such that

$$\min_{\mathbf{S} \in \mathcal{S}_{\infty}, \mathbf{S} \neq \mathbf{0}} \{ |\det(\mathbf{S})|^2 \} = c > 0$$

for some constant  $c$ . Let the  $\mathbb{F}$ -basis  $\{\theta_i, i = 1, \dots, n_t\}$  be such that all the  $\theta_i$  belong to  $\mathcal{O}_{\mathbb{K}}$ . Since  $\gamma \in \mathbb{F}$  and satisfies (5), we can express  $\gamma$  as  $\gamma = \frac{a}{b}$  with  $a, b \in \mathcal{O}_{\mathbb{F}} \setminus \{0\}$ . Now, multiplying all the matrices of  $\mathcal{S}_{\infty}$  by  $b$  results in all the entries of all the matrices of  $\mathcal{S}_{\infty}$  belonging to  $\mathcal{O}_{\mathbb{K}}$  and from (6), any nonzero matrix of  $\mathcal{S}_{\infty}$  has a determinant that belongs to  $(\mathbb{F} \cap \mathcal{O}_{\mathbb{K}}) \setminus \{0\} = \mathcal{O}_{\mathbb{F}} \setminus \{0\}$ . Since  $\mathcal{O}_{\mathbb{F}}$  is either  $\mathbb{Z}[i]$  or  $\mathbb{Z}[\omega]$ , we have

$$\min_{\mathbf{S} \in \mathcal{S}_{\infty}, \mathbf{S} \neq \mathbf{0}} \{ |\det(\mathbf{S})|^2 \} \geq \frac{1}{|b|^{2n_t}} > 0$$

which proves the proposition.  $\blacksquare$

So, for the purpose of space-time coding, an  $\mathbb{F}$ -basis  $\{\theta_i, i = 1, 2, \dots, n_t \mid \theta_i \in \mathcal{O}_{\mathbb{K}}\}$  is chosen (this can also be an  $\mathcal{O}_{\mathbb{F}}$ -basis of  $\mathcal{O}_{\mathbb{K}}$ ) and the  $a_i \in \mathbb{K}$  in (3) are expressed as linear combinations of elements of this basis over  $\mathcal{O}_{\mathbb{F}}$ . The STBC which encodes symbols from a complex constellation  $\mathcal{A}_q$  ( $M$ -QAM or  $M$ -HEX) has its codewords of the form shown in (3) with  $a_i = \sum_{j=1}^{n_t} s_{ij} \theta_j$ ,  $s_{ij} \in \mathcal{A}_q \subset \mathcal{O}_{\mathbb{F}}$  with  $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$  or  $\mathbb{Z}[\omega]$ . A codeword matrix of STBCs from CDA has  $n_t$

layers [1], with the  $(i+1)^{th}$  layer transmitting the vector  $\mathbf{D}_i[a_i, \tau(a_i), \dots, \tau^{n-1}(a_i)]^T$ ,  $i = 0, \dots, n_t - 1$ , where

$$\mathbf{D}_i \triangleq \text{diag}[\underbrace{1, \dots, 1}_{n_t-i \text{ times}}, \underbrace{\gamma, \dots, \gamma}_i] \quad (7)$$

and  $[a_i, \tau(a_i), \dots, \tau^{n-1}(a_i)]^T = \mathbf{R} \mathbf{s}_i$ ,  $i = 0, \dots, n_t - 1$ , where  $\mathbf{s}_i = [s_{i1}, s_{i2}, \dots, s_{in_t}]^T \in \mathcal{A}_q^{n_t \times 1}$  and  $\mathbf{R} \in \mathbb{C}^{n_t \times n_t}$  is the *generator matrix* of each layer of the STBC (not to be confused with the generator matrix  $\mathbf{G}$  of the STBC which is given by Definition 4) and is given as

$$\mathbf{R} = \frac{1}{\sqrt{\lambda}} \begin{bmatrix} \theta_1 & \cdots & \theta_{n_t} \\ \tau(\theta_1) & \cdots & \tau(\theta_{n_t}) \\ \vdots & \vdots & \vdots \\ \tau^{n-1}(\theta_1) & \cdots & \tau^{n-1}(\theta_{n_t}) \end{bmatrix} \quad (8)$$

where, as mentioned earlier,  $\{\theta_i, i = 1, 2, \dots, n_t \mid \theta_i \in \mathcal{O}_{\mathbb{K}}\}$  is an  $\mathbb{F}$ -basis of  $\mathbb{K}$  and  $\lambda$  is a suitable real-valued scalar designed so that the STBC meets the energy constraint in (2).

### C. Perfect Codes

The perfect STBCs are designed to be equipped with the following two desirable properties [1], [3].

- *Approximate-universality* : This is achieved if the STBC satisfies the following criteria.

- C1 *Full-rate*<sup>1</sup> : The STBC transmits  $n_t^2$  independent complex information symbols in  $n_t$  channel uses.
- C2 *Non-vanishing determinant* : The STBC-scheme has the NVD property.

- *Energy-efficiency/coding gain* : To achieve this, the STBC should satisfy the following criteria.

- C3 *Constellation shaping criterion* : The matrix  $\mathbf{R}$  given by (8) is unitary [1] so that on each layer, the energy required to transmit the linear combination of information symbols is equal to the energy required to transmit the information symbols themselves, i.e.,  $\|\mathbf{R} \mathbf{s}_i\|^2 = \|\mathbf{s}_i\|^2$ ,  $i = 0, \dots, n_t - 1$ , with the notations as used in the previous subsection.
- C4 *Uniform average transmitted energy* : The average transmitted energy for all the antennas in all time slots is the same.

To satisfy C1,  $\mathbb{F}$  is chosen to be  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\omega)$  and a CDA of degree  $n_t$  over  $\mathbb{F}$  is constructed. C2 is satisfied by choosing an  $\mathbb{F}$ -basis  $\{\theta_i, i = 1, 2, \dots, n_t \mid \theta_i \in \mathcal{O}_{\mathbb{K}}\}$  which guarantees a non-vanishing determinant from Proposition 1.

<sup>1</sup>In this paper, a rate- $n_t$  STBC is referred to as a full-rate STBC.

C3 is satisfied by choosing the  $\mathbb{F}$ -basis  $\{\theta_i, i = 1, 2, \dots, n_t \mid \theta_i \in \mathcal{O}_{\mathbb{K}}\}$  such that  $\mathbf{R}$  is unitary. C4 is satisfied by choosing  $\gamma$  such that  $|\gamma|^2 = 1$ . In [1],  $\gamma$  is chosen to be in  $\mathbb{F}$  while in [3],  $\gamma$  is chosen to be the ratio of a suitable element  $a \in \mathcal{O}_{\mathbb{F}} \setminus \{0\}$  and its complex conjugate. In the former case, the minimum determinant, prior to normalization, is a nonzero positive integer while in the latter case, it is  $\frac{1}{|a|^{2(n_t-1)}}$  [3]. Choosing  $\gamma$  to be in  $\mathbb{F}$  restricts the construction of the perfect STBCs to only 2, 3, 4 and 6 transmit antennas [1] but these STBCs have the largest known coding gains in their class<sup>2</sup>.

### III. MODIFIED SHAPING CRITERION

For an STBC that is obtained from CDA to be energy efficient, C3, which asks for  $\mathbf{R}$  to be unitary, is a sufficient but not a necessary criterion - it is not necessary that on the  $i^{\text{th}}$  layer, the energy required to transmit  $a_{i-1}$ ,  $\tau(a_{i-1})$ ,  $\dots$ , and  $\tau^{n_t-1}(a_{i-1})$  be equal to the energy used for sending the information symbols  $s_{ij}$  themselves. It is sufficient that the *average* energy required to send the linear combination of the information symbols on each layer is equal to the *average* energy used for sending the information symbols themselves, i.e.,  $\mathbb{E}(\|\mathbf{R}\mathbf{s}_i\|^2) = \mathbb{E}(\|\mathbf{s}_i\|^2)$ ,  $i = 0, \dots, n_t - 1$  (with the notations as in Subsection II-B), where the expectation is over the distribution of  $\mathbf{s}_i$  which by assumption has probability mass function (PMF) given by  $p_{s_i}(\mathbf{s}) = (1/M)^{n_t}$ ,  $\forall \mathbf{s} \in \mathcal{A}_q^{n_t \times 1}$ . Hence, unitariness of  $\mathbf{R}$  is not necessary. However, in literature, a unitary  $\mathbf{R}$  is seen as desirable as it makes the STBC information-lossless. We elaborate on this in the following subsection.

#### A. Unitary generator matrix $\mathbf{G}$ and information-losslessness

An STBC is said to be *information-lossless* [9] if the maximum instantaneous mutual information of the equivalent MIMO channel after space-time processing is the same as the maximum instantaneous mutual information of the MIMO channel without space-time processing. The maximum instantaneous mutual information (in bits per channel use) supported by the MIMO channel without an STBC encoder is [13]

$$C(\mathbf{H}) = \max_{\text{tr}(\mathbf{Q}) \leq \rho} \log_2 \det(\mathbf{I} + \mathbf{H}\mathbf{Q}\mathbf{H}^H)$$

where  $\mathbf{Q}$  is a non-negative definite matrix. A good approximation for  $\mathbf{Q}$  is taken<sup>3</sup> to be  $(\rho/n_t)\mathbf{I}$  so that

$$C(\mathbf{H}) \approx \log_2 \det\left(\mathbf{I} + \frac{\rho}{n_t} \mathbf{H}\mathbf{H}^H\right). \quad (9)$$

Now, for linear STBCs of the form  $\mathcal{S} = \{\sum_{i=1}^k s_i \mathbf{A}_i\}$ , the signal model given in (1) can be rewritten as

$$\text{vec}(\mathbf{Y}) = \rho(\mathbf{I}_T \otimes \mathbf{H})\mathbf{G}\mathbf{s} + \text{vec}(\mathbf{N})$$

<sup>2</sup>There are certain non-linear STBCs, for example in [12], which beat the Golden code. These STBCs employ spherical shaping, involve additional complexity in encoding and are not sphere-decodable. We do not consider this class of non-linear STBCs in this paper.

<sup>3</sup>For calculating the ergodic capacity which is the expectation of  $C(\mathbf{H})$  over  $\mathbf{H}$ ,  $(\rho/n_t)\mathbf{I}$  is the optimal  $\mathbf{Q}$ .

where  $\mathbf{I}_T$  is the identity matrix of size  $T \times T$ ,  $\mathbf{G}$  is the generator matrix defined in Definition 4 and  $\mathbf{s}$  is the vector of information symbols belonging to  $\mathcal{A}_q^{k \times 1}$ . For this model, the maximum mutual information for a given channel matrix  $\mathbf{H}$  is

$$C'(\mathbf{H}) = \max_{\text{tr}(\mathbf{G}\mathbf{Q}'\mathbf{G}^H) \leq \rho T} \left( \frac{1}{T} \log_2 \det(\mathbf{I} + \bar{\mathbf{H}}\mathbf{G}\mathbf{Q}'\mathbf{G}^H\bar{\mathbf{H}}^H) \right)$$

where  $\mathbf{Q}'$  is non-negative definite and  $\bar{\mathbf{H}} = \mathbf{I}_T \otimes \mathbf{H}$ . When  $\mathbf{G}$  is unitary (possible only when  $k = n_t T$ ) and  $\mathbf{Q}' = (\rho/n_t)\mathbf{I}$ ,  $C'(\mathbf{H})$  is equal to  $C(\mathbf{H})$  (assuming  $C(\mathbf{H})$  is equal to the right hand side of (9)) and hence the STBC is information-lossless [5], [9]. For STBCs from CDA, if  $\mathbf{R}$  given by (8) is unitary, so is  $\mathbf{G}$ .

However, it is important to note that the expressions for both  $C(\mathbf{H})$  and  $C'(\mathbf{H})$  are obtained for *Gaussian inputs* (since the entropy of the output is maximized if and only if the input is Gaussian). In the case of STBCs, the inputs information symbols take values from  $\mathcal{A}_q$  which is  $M$ -QAM or  $M$ -HEX, and all the signal points are equally likely to be chosen so that the PMF of  $s_i$  is  $p_{s_i}(s) = 1/M$ ,  $\forall s \in \mathcal{A}_q$ . So, for the signal model  $\mathbf{y} = \rho\mathbf{H}\mathbf{s} + \mathbf{n}$  where  $\mathbf{s} \in \mathcal{A}_q^{n_t \times 1}$ , the constellation constrained mutual information  $C_c(\mathbf{H})$  is not given by (9) but by the following expression [14], [15].

$$C_c(\mathbf{H}) = -\mathbb{E} \log_2 \left( \frac{1}{(M\pi)^{n_t}} \sum_{\mathbf{s} \in \mathcal{A}_q^{n_t \times 1}} e^{-\frac{\|\mathbf{y} - \rho\mathbf{H}\mathbf{s}\|^2}{\pi^{n_t}}} \right) - n_t \log_2(\pi e) \quad (10)$$

where the expectation is over the distribution of  $\mathbf{y}$ . With space time coding, the corresponding constellation constrained mutual information is

$$C'_c(\mathbf{H}) = -\frac{1}{T} \mathbb{E} \log_2 \left( \frac{1}{(M\pi)^{n_t T}} \sum_{\mathbf{s} \in \mathcal{A}_q^{n_t T \times 1}} e^{-\frac{\|\mathbf{y}' - \rho\bar{\mathbf{H}}\mathbf{G}\mathbf{s}\|^2}{\pi^{n_t T}}} \right) - n_t \log_2(\pi e) \quad (11)$$

where  $\mathbf{y}' = \text{vec}(\mathbf{Y})$  and the expectation is over the distribution of  $\mathbf{y}'$ . It is clear from (10) and (11) that the significance of unitariness of the generator matrix  $\mathbf{G}$  is questionable when discrete constellations are used. In particular, the notion of information-lossless STBCs is itself questionable.

#### B. Modified Shaping criterion

Having noted that unitariness of  $\mathbf{G}$  and hence of  $\mathbf{R}$  is not a necessary criterion, we propose a change in C3 as follows. The modified shaping criterion can be separated into two subcriteria which are

- C3.1 the *average* energy required to transmit the linear combination of the information symbols on each layer is equal to the *average* energy used for sending the information symbols themselves, i.e.,  $\mathbb{E}(\|\mathbf{R}\mathbf{s}_i\|^2) = \mathbb{E}(\|\mathbf{s}_i\|^2)$ ,  $i = 0, \dots, n_t - 1$ , where the expectation is over the distribution of  $\mathbf{s}_i$  which by assumption has a PMF given by  $p_{s_i}(\mathbf{s}) = (1/M)^{n_t}$ ,  $\forall \mathbf{s} \in \mathcal{A}_q^{n_t \times 1}$ .
- C3.2 All the  $n_t^2$  symbols are transmitted at the same average energy.



The rationale behind C3.1 is obvious - we do not wish to blow up the average energy required to transmit the information symbols. The reason for coming up with C3.2 is that no symbol should be favoured over other symbols with respect to energy required for transmission. We assume that the average energy of  $\mathcal{A}_Q$  is  $E$  so that  $\mathbb{E}(\|\mathbf{s}_i\|^2) = n_t E$  and  $\mathbb{E}(\mathbf{s}_i \mathbf{s}_i^H) = E \mathbf{I}$ . It is also assumed that  $|\gamma|^2 = 1$  so that  $\mathbf{D}_i$  given by (7) is unitary, since it is a necessary condition for C4 to be satisfied. With these assumptions, we have the following proposition.

*Proposition 2:* C3.1, C3.2 and C4 are together satisfied if and only if  $\mathbf{R}$  given by (8) is such that all of its rows and columns have a Euclidean norm equal to unity.

*Proof:* We prove that if C3.1, C3.2 and C4 are together satisfied, then  $\mathbf{R}$  shall be such that all of its rows and columns have a Euclidean norm equal to unity. The converse is then easy to see. If C3.1 is satisfied, then, with  $\mathbf{D}_i$  unitary, we have

$$\begin{aligned} \mathbb{E}(\|\mathbf{s}_i\|^2) &= \mathbb{E}(\|\mathbf{D}_i \mathbf{R} \mathbf{s}_i\|^2) = \mathbb{E}[\text{tr}(\mathbf{R} \mathbf{s}_i (\mathbf{R} \mathbf{s}_i)^H)] \\ &= \mathbb{E}[\text{tr}(\mathbf{R} \mathbf{s}_i \mathbf{s}_i^H \mathbf{R}^H)] = \text{tr}[\mathbb{E}(\mathbf{R} \mathbf{s}_i \mathbf{s}_i^H \mathbf{R}^H)] \\ &= \text{tr}[\mathbf{R} \mathbb{E}(\mathbf{s}_i \mathbf{s}_i^H) \mathbf{R}^H] = \text{tr}[\mathbf{R} (E \mathbf{I}) \mathbf{R}^H] \\ &= E \sum_{i=1}^{n_t} \|\mathbf{r}_i\|^2 \end{aligned} \quad (12)$$

where  $\mathbf{r}_i$  denotes the  $i^{\text{th}}$  row of  $\mathbf{R}$ . It follows that for C4 to be satisfied,

$$\mathbb{E}(\|\mathbf{r}_1 \mathbf{s}_i\|^2) = \mathbb{E}(\|\mathbf{r}_2 \mathbf{s}_i\|^2) = \dots = \mathbb{E}(\|\mathbf{r}_{n_t} \mathbf{s}_i\|^2), \quad (13)$$

$\forall i = 0, \dots, n_t - 1$ . So, from (12), (13) and the fact that  $\mathbb{E}(\|\mathbf{s}_i\|^2) = n_t E$ ,  $\mathbf{R}$  must satisfy  $\|\mathbf{r}_1\|^2 = \|\mathbf{r}_2\|^2 = \dots = \|\mathbf{r}_{n_t}\|^2 = 1$ . Now, denoting the  $i^{\text{th}}$  column of  $\mathbf{R}$  by  $\mathbf{r}'_i$ , we have

$$\begin{aligned} \mathbb{E}(\|\mathbf{s}_i\|^2) &= \mathbb{E}(\|\mathbf{D}_i \mathbf{R} \mathbf{s}_i\|^2) = \mathbb{E}(\|\mathbf{R} \mathbf{s}_i\|^2) \\ &= \mathbb{E}[\mathbf{s}_i^H \mathbf{R}^H \mathbf{R} \mathbf{s}_i] = E \sum_{i=1}^{n_t} \|\mathbf{r}'_i\|^2. \end{aligned}$$

But C3.2 demands that  $\|\mathbf{r}'_1\|^2 = \|\mathbf{r}'_2\|^2 = \dots = \|\mathbf{r}'_{n_t}\|^2$ . Hence, the Euclidean norm of each row and column of  $\mathbf{R}$  should be equal to unity. This concludes the proof. ■

An STBC with a unitary matrix  $\mathbf{R}$  obviously satisfies the modified shaping criterion but unitariness is not a necessary condition. In the following two sections, we highlight the significance of the modified shaping criterion by showing the existence of STBCs which do not have a unitary  $\mathbf{R}$  but have a higher coding gain than the perfect STBCs for 4 and 6 transmit antennas [1] which were so far unbeaten in this regard. We call these STBCs “improved perfect STBCs” and they are formally defined as follows.

*Definition 5: (Improved perfect STBC) :* An STBC that satisfies C1, C2, C3.1, C3.2 and C4, and has a larger normalized minimum determinant than the existing best comparable perfect STBC is called an improved perfect STBC.

#### IV. IMPROVED PERFECT STBC FOR 4 TX

The improved perfect STBC for 4 transmit antennas, which we call  $\mathcal{C}_4$ , was first reported in [4] but its superior coding gain went unnoticed.  $\mathcal{C}_4$  is obtained from the CDA  $\mathcal{A} =$

$(\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i), \tau : \zeta_5 \mapsto \zeta_5^2, i)$  [4], with  $\zeta_5$  being the primitive 5<sup>th</sup> root of unity. Its codeword matrix, prior to normalization, has the structure

$$\mathbf{S} = \begin{bmatrix} a_0 & i\tau(a_3) & i\tau^2(a_2) & i\tau^3(a_1) \\ a_1 & \tau(a_0) & i\tau^2(a_3) & i\tau^3(a_2) \\ a_2 & \tau(a_1) & \tau^2(a_0) & i\tau^3(a_3) \\ a_3 & \tau(a_2) & \tau^2(a_1) & \tau^3(a_0) \end{bmatrix}$$

where  $a_i = s_{i1} + s_{i2}\zeta_5 + s_{i3}\zeta_5^2 + s_{i4}\zeta_5^3$ ,  $i = 0, 1, 2, 3$  and  $s_{ij} \in M$ -QAM. Clearly,  $\mathcal{C}_4$  satisfies C1. The  $\mathbb{Q}(i)$ -basis is  $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$  which is also a  $\mathbb{Z}[i]$ -basis [16, p. 158] for  $\mathbb{Z}[i, \zeta_5]$  and  $\mathbf{R}$ , as defined in (8), is

$$\frac{1}{2} \begin{bmatrix} 1 & \zeta_5 & \zeta_5^2 & \zeta_5^3 \\ 1 & \zeta_5^2 & \zeta_5^4 & \zeta_5 \\ 1 & \zeta_5^4 & \zeta_5^3 & \zeta_5^2 \\ 1 & \zeta_5^3 & \zeta_5 & \zeta_5^4 \end{bmatrix}.$$

It is clear that the modified shaping criterion is satisfied. Noting that  $\gamma = i$  has unit modulus,  $\mathcal{C}_4$  satisfies C4 as well. It only remains to be seen whether C2 is satisfied. Although this is shown in [4], we provide our version of the proof here for the sake of completeness and the steps of this proof will be used in the next section where the STBC for 6 transmit antennas is discussed. We first show that  $(\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i), \tau : \zeta_5 \mapsto \zeta_5^2, i)$  is a division algebra and subsequently, application of Proposition 1 establishes that the NVD criterion is satisfied.

*Proposition 3:*  $\mathcal{A} = (\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i), \tau : \zeta_5 \mapsto \zeta_5^2, i)$  is a division algebra.

*Proof:* To prove that  $\mathcal{A}$  is a CDA, it is sufficient to show that  $N_{\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)}(a) = \prod_{j=0}^3 \tau^j(a) \neq i^t$ ,  $t = 1, 2, 3$ ,  $\forall a \in \mathbb{Q}(i, \zeta_5)$ . Thus, we have to establish that  $i$ ,  $-1$  and  $-i$  are not norms in  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$ . Noting that  $\zeta_5 + \zeta_5^{-1} = (-1 + \sqrt{5})/2$ , it is clear that  $\mathbb{Q}(i, \sqrt{5}) \subset \mathbb{Q}(i, \zeta_5)$ . Since  $[\mathbb{Q}(i, \zeta_5) : \mathbb{Q}(i)] = 4$  and  $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}(i)] = 2$ , by the multiplicative formula for tower of fields,  $[\mathbb{Q}(i, \zeta_5) : \mathbb{Q}(i, \sqrt{5})] = 2$  and  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i, \sqrt{5})$  is a Galois extension of degree 2. Further, since  $\zeta_5^4 = \zeta_5^{-1}$ ,  $\tau^2(\zeta_5 + \zeta_5^{-1}) = \zeta_5^{-1} + \zeta_5$  and  $\tau^2$  fixes  $\mathbb{Q}(i, \sqrt{5})$ . So,  $\text{Gal}(\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i, \sqrt{5})) = \{1, \tau^2\}$  and  $\text{Gal}(\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)) = \{1, \tau_{|\mathbb{Q}(i, \sqrt{5})}\}$ , where  $\tau_{|\mathbb{Q}(i, \sqrt{5})}$  denotes “ $\tau$  restricted to  $\mathbb{Q}(i, \sqrt{5})$ ”. So, if  $i$  were a norm in  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$ , then for some  $a$  in  $\mathbb{Q}(i, \zeta_5)$ ,

$$\begin{aligned} i &= a\tau(a)\tau^2(a)\tau^3(a) \\ &= (a\tau^2(a))\tau(a\tau^2(a)). \end{aligned} \quad (15)$$

But  $a\tau^2(a)$  is invariant under  $\tau^2$  and hence belongs to  $\mathbb{Q}(i, \sqrt{5})$ . So, (15) implies that  $i$  is a norm in  $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$  which is not true [8] since  $(\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \tau : \sqrt{5} \mapsto -\sqrt{5}, i)$  is a division algebra. Therefore,  $i$  is not a norm in  $\mathbb{Q}(i, \zeta_5)$ . Likewise,  $-i$  is also not a norm in  $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$  (for if  $a\tau(a) = -i$ , then  $(ia)\tau(ia) = i$  for some  $a \in \mathbb{Q}(i, \sqrt{5})$  which is a contradiction) and hence not a norm in  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$ .

Now, it only remains to be seen that  $-1$  is not a norm in  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$ . This is proved using class field theory whose usage in proving that a unit is not a norm in the extension field is provided in [1, Appendix II]. In [1, Appendix IV], it is shown that  $-1$  is not a norm in  $\mathbb{Q}(i, 2 \cos(\frac{2\pi}{15}))/\mathbb{Q}(i)$ . The

$$\mathbf{S} = \begin{bmatrix} a_0 & -\omega\tau(a_5) & -\omega\tau^2(a_4) & -\omega\tau^3(a_3) & -\omega\tau^4(a_2) & -\omega\tau^5(a_1) \\ a_1 & \tau(a_0) & -\omega\tau^2(a_5) & -\omega\tau^3(a_4) & -\omega\tau^4(a_3) & -\omega\tau^5(a_2) \\ a_2 & \tau(a_1) & \tau^2(a_0) & -\omega\tau^3(a_5) & -\omega\tau^4(a_4) & -\omega\tau^5(a_3) \\ a_3 & \tau(a_2) & \tau^2(a_1) & \tau^3(a_0) & -\omega\tau^4(a_5) & -\omega\tau^5(a_4) \\ a_4 & \tau(a_3) & \tau^2(a_2) & \tau^3(a_1) & \tau^4(a_0) & -\omega\tau^5(a_5) \\ a_5 & \tau(a_4) & \tau^2(a_3) & \tau^3(a_2) & \tau^4(a_1) & \tau^5(a_0) \end{bmatrix} \quad (14)$$

discriminant (see Appendix I of this paper) of  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$  is  $5^3\mathbb{Z}[i]$ . The only prime ideals in  $\mathbb{Z}[i]$  that are ramified in  $\mathbb{Q}(i, \zeta_5)$  are the ones that divide  $125\mathbb{Z}[i]$  and hence divide  $5\mathbb{Z}[i]$ . These are precisely the prime ideals  $(2+i)\mathbb{Z}[i]$  and  $(2-i)\mathbb{Z}[i]$ . With these facts, the same proof given in [1, Appendix IV], with 2 minor changes, establishes that  $-1$  is not a norm in  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$ . The first minor change is that we need to establish that the prime ideal  $(-25+12i)\mathbb{Z}[i]$  does not completely split in  $\mathbb{Z}[i, \zeta_5]$ , whereas in [1, Appendix IV],  $(-25+12i)\mathbb{Z}[i]$  was required not to be completely split in the ring of integers of  $\mathbb{Q}(i, 2\cos\frac{2\pi}{15})$ . This is proven in Appendix II. The second change from the proof in [1, Appendix IV] is that  $3\mathbb{Z}[i]$  is not ramified in  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$  and need not be taken into consideration for evaluating the Hasse norm symbol at ramified places. ■

#### A. Minimum determinant

The entries of all the codewords of  $\mathcal{C}_4$ , prior to normalization of  $\mathbf{R}$  by  $1/2$ , belong to  $\mathbb{Z}[i, \zeta_5]$ , the ring of integers in  $\mathbb{Q}(i, \zeta_5)$ , and hence the determinant of any codeword difference matrix belongs to  $\mathbb{Z}[i, \zeta_5]$ . From (6), the determinant of any codeword difference matrix belongs to  $\mathbb{Q}(i) \cap \mathbb{Z}[i, \zeta_5] = \mathbb{Z}[i]$  and so, the minimum determinant is at least 1. But when the symbols take values from  $M$ -QAM with an average energy of  $E$  units, the difference between any two symbols is a multiple of 2. Taking into account a scaling factor of  $\frac{1}{4\sqrt{E}}$  so that the expectation of the square of the Euclidean norm of each column of the codeword matrices is unity<sup>4</sup> (see Definition 1), the normalized minimum determinant of  $\mathcal{C}_4$  is  $\left(\frac{2}{4\sqrt{E}}\right)^8 = \frac{1}{256E^4}$  which is significantly larger than the normalized minimum determinant of the perfect STBC for 4 transmit antennas that stands at  $\frac{1}{1125E^4}$  [1]. A result of this larger minimum determinant is a superior error performance compared to the perfect STBC and this is evident in Fig. 1 which gives a comparison of the error performance of the two STBCs for 4-QAM.

#### V. $\mathcal{C}_6$ - IMPROVED PERFECT STBC FOR 6 TX

$\mathcal{C}_6$  is obtained from the algebra  $\mathcal{A} = (\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega), \tau : \zeta_7 \mapsto \zeta_7^3, -\omega)$  with  $\zeta_7$  being the primitive 7<sup>th</sup> root of unity. Its codeword matrix has the structure shown in (14) at the top of the page with  $a_i = s_{i1} + s_{i2}\zeta_7 + s_{i3}\zeta_7^2 + s_{i4}\zeta_7^3 + s_{i5}\zeta_7^4 + s_{i6}\zeta_7^5$ ,  $i = 0, 1, 2, \dots, 5$ , and  $s_{ij} \in M$ -HEX. Clearly,  $\mathcal{C}_6$  is full-rate

<sup>4</sup>For STBCs like the perfect STBCs, the average energy for transmission of symbols in each time slot is uniform and the energy constraint (2) translates to the requirement that the expectation of the square of the Euclidean norm of each column of codeword matrices be unity.

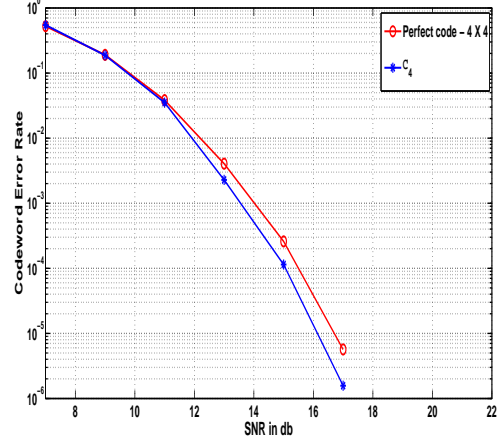


Fig. 1. CER performance of the Perfect STBC and  $\mathcal{C}_4$  for the  $4 \times 4$  system with 4-QAM

since  $\{1, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5\}$  is a  $\mathbb{Z}[\omega]$ -basis for  $\mathbb{Z}[\omega, \zeta_7]$ .  $\mathbf{R}$  (as defined in (8)) is

$$\frac{1}{\sqrt{6}} \begin{bmatrix} 1 & \zeta_7 & \zeta_7^2 & \zeta_7^3 & \zeta_7^4 & \zeta_7^5 \\ 1 & \zeta_7^3 & \zeta_7^6 & \zeta_7^2 & \zeta_7^5 & \zeta_7 \\ 1 & \zeta_7^2 & \zeta_7^4 & \zeta_7^6 & \zeta_7 & \zeta_7^3 \\ 1 & \zeta_7^6 & \zeta_7^5 & \zeta_7^4 & \zeta_7^3 & \zeta_7^2 \\ 1 & \zeta_7^4 & \zeta_7 & \zeta_7^5 & \zeta_7^2 & \zeta_7^6 \\ 1 & \zeta_7^5 & \zeta_7^3 & \zeta_7 & \zeta_7^6 & \zeta_7^4 \end{bmatrix}$$

and it is clear that the norm of each row and column of  $\mathbf{R}$  is equal to 1. Noting that  $\gamma = -\omega$  has unit modulus,  $\mathcal{C}_6$  satisfies both the modified shaping criterion and C4. To show that the NVD criterion is also satisfied, it is sufficient to show that  $(\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega), \tau : \zeta_7 \mapsto \zeta_7^3, -\omega)$  is a division algebra following which the application of Proposition 1 establishes that the NVD criterion is satisfied.

**Proposition 4:**  $\mathcal{A} = (\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega), \tau : \zeta_7 \mapsto \zeta_7^3, -\omega)$  is a division algebra.

**Proof:** To prove that  $\mathcal{A}$  is a CDA, it is sufficient to show that  $N_{\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)}(a) = \prod_{j=0}^5 \tau^j(a) \neq (-\omega)^t$ ,  $t = 1, 2, \dots, 5$ ,  $\forall a \in \mathbb{Q}(\omega, \zeta_7)$ . Hence, it is to be established that  $\pm\omega, \pm\omega^2, -1$  are not norms in  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$ . We note that  $\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1}) \subset \mathbb{Q}(\omega, \zeta_7)$ . Since  $[\mathbb{Q}(\omega, \zeta_7) : \mathbb{Q}(\omega)] = 6$  and  $[\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1}) : \mathbb{Q}(\omega)] = 3$ , by the multiplicative formula for tower of fields,  $[\mathbb{Q}(\omega, \zeta_7) : \mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})] = 2$  and  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})$  is a Galois extension of degree 2. Further,  $\tau^3(\zeta_7 + \zeta_7^{-1}) = \zeta_7^{-1} + \zeta_7$  (since  $\zeta_7^{-1} = \zeta_7^6$ ) and  $\tau^3$  fixes  $\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})$ . So,  $\text{Gal}(\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})) = \{1, \tau^3\}$  and  $\text{Gal}(\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\omega)) = \{1, \tau|_{\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})}, \tau^2|_{\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})}\}$ . So, if  $\pm\omega$

# Tx antennas	STBC	Constellation (average energy $E$ )	$\delta_{min}$	Approximately Universal?
4	Perfect Code [1]	QAM	$\frac{1}{1125E^4}$	Yes
	$\mathcal{C}_4$ [4]	QAM	$\frac{1}{256E^4}$	Yes
6	Perfect STBC [1]	HEX	$\frac{1}{3^6 7^5 E^6} \leq \delta_{min} \leq \frac{1}{3^6 7^4 E^6}$	Yes
	$\mathcal{C}_6$	HEX	$\frac{1}{3^{12} E^6}$	Yes

TABLE I  
COMPARISON OF OUR STBCs WITH KNOWN BEST STBCs.

were a norm in  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$ , then for some  $a$  in  $\mathbb{Q}(\omega, \zeta_7)$ ,

$$\begin{aligned} \pm \omega &= a\tau(a)\tau^2(a)\tau^3(a)\tau^4(a)\tau^5(a) \\ &= (a\tau^3(a))\tau(a\tau^3(a))\tau^2(a\tau^3(a)). \end{aligned} \quad (16)$$

But  $a\tau^3(a)$  is invariant under  $\tau^3$  and hence belongs to  $\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})$ . So, (16) implies that  $\omega$  is a norm in  $\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\omega)$  which is not true [8] since  $(\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\omega), \tau : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}, \omega)$  is a division algebra ( $-\omega$  not being a norm naturally follows). Therefore,  $\pm\omega$  is not a norm in  $\mathbb{Q}(\omega, \zeta_7)$ . Likewise,  $\pm\omega^2$  is also not a norm in  $\mathbb{Q}(\omega, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\omega)$  and hence not a norm in  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$ .

Now, it only remains to be seen that  $-1$  is not a norm in  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$ . This is again proved using class field theory. In [1, Appendix V], it is shown that  $-1$  is not a norm in  $\mathbb{Q}((\omega, 2\cos(\frac{2\pi}{28}))/\mathbb{Q}(\omega))$ . The discriminant of  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$  is  $7^5\mathbb{Z}[\omega]$ . The only prime ideals in  $\mathbb{Z}(\omega)$  that are ramified in  $\mathbb{Q}(\omega, \zeta_7)$  are the ones that divide  $7^5\mathbb{Z}[\omega]$  and hence divide  $7\mathbb{Z}[\omega]$ . These are precisely the prime ideals  $(3+\omega)\mathbb{Z}[\omega]$  and  $(2-\omega)\mathbb{Z}[\omega]$ . Using these facts, the same proof given in [1, Appendix V], with 2 minor changes, establishes that  $-1$  is not a norm in  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$ . The first change is that we are required to show that the prime ideal  $(3-8\omega)\mathbb{Z}[\omega]$  is not completely split in  $\mathbb{Z}[\omega, \zeta_7]$ , whereas in [1, Appendix V],  $(3-8\omega)\mathbb{Z}[\omega]$  was required to be not completely split in the ring of integers of  $\mathbb{Q}(\omega, 2\cos\frac{2\pi}{28})$ . It is shown in Appendix III of this paper that  $(3-8\omega)\mathbb{Z}[\omega]$  is not completely split in  $\mathbb{Z}[\omega, \zeta_7]$ . The second change from the proof in [1, Appendix V] is that  $2\mathbb{Z}[\omega]$  is not ramified in  $\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega)$  and need not be taken into consideration for evaluating the Hasse norm symbol at ramified places. ■

#### A. Minimum Determinant

The entries of all the codewords of  $\mathcal{C}_6$ , prior to normalization of  $\mathbf{R}$  by  $1/\sqrt{6}$ , belong to  $\mathbb{Z}[\omega, \zeta_7]$ , the ring of integers of  $\mathbb{Q}(\omega, \zeta_7)$ , and hence the determinant of any codeword difference matrix belongs to  $\mathbb{Q}(\omega) \cap \mathbb{Z}[\omega, \zeta_7] = \mathbb{Z}[\omega]$ . So, the minimum determinant is guaranteed to be at least 1. But since the symbols take values from  $M$ -HEX with an average energy of  $E$  units, the difference between any two symbols is a multiple of 2. Taking into account a normalizing factor of  $\frac{1}{6\sqrt{E}}$ , the normalized minimum determinant of  $\mathcal{C}_6$

is  $\left(\frac{2}{6\sqrt{E}}\right)^{12} = \frac{1}{3^{12}E^6}$  which is significantly larger than the normalized minimum determinant of the perfect STBC for 6 transmit antennas that is upper bounded by  $\frac{1}{3^6 7^4 E^6}$  [1]. The normalized minimum determinants of the improved perfect STBCs and the perfect STBCs are tabulated in Table I.

*Remarks:* We have restricted our construction of the improved perfect STBCs to just 4 and 6 transmit antennas. The usage of cyclotomic extensions of  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\omega)$  was the reason we were able to obtain STBCs with larger normalized minimum determinants than that of perfect STBCs for 4 and 6 transmit antennas. However, for  $n_t = 2, 3$ , one cannot obtain CDAs of degree  $n_t$  over  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\omega)$  using cyclotomic extensions (with  $\zeta_3 = \omega$ ,  $(\mathbb{Q}(i, \omega)/\mathbb{Q}(i), \tau : \omega \rightarrow \omega^2, i)$  is not a division algebra). So, for 2 and 3 transmit antennas, the existing perfect STBCs [1] remain the best with respect to coding gain. For other values of  $n_t$ ,  $\gamma$  cannot be a unit in  $\mathbb{Z}[i]$  or  $\mathbb{Z}[\omega]$  for the algebra to be a division algebra. However, the approach taken in [3], where  $\gamma$  is not restricted to be in  $\mathbb{Z}[i]$  or  $\mathbb{Z}[\omega]$ , can still be taken to investigate if new STBCs with larger coding gains can be obtained for arbitrary number of transmit antennas.

## VI. CONCLUDING REMARKS

In this paper, we presented a modified shaping criterion in the design of STBCs that enabled us to propose two STBCs, one each for 4 and 6 transmit antennas, that have the best known normalized minimum determinants in their class. This shaping criterion can be employed to see if better STBCs, in terms of coding gain, can be obtained for arbitrary number of transmit antennas.

## APPENDIX I

### NUMBER THEORY BASICS AND DEFINITIONS

We consider a number field  $\mathbb{F}$  that is a finite extension of  $\mathbb{Q}$ . Its ring of integers  $\mathcal{O}_{\mathbb{F}}$  is given by  $\mathcal{O}_{\mathbb{F}} = \{a \in \mathbb{F} \mid f(a) = 0, f \in \mathbb{Z}_{monic}[X]\}$  where  $\mathbb{Z}_{monic}[X]$  is the set of monic polynomials in the variable  $X$  with coefficients in  $\mathbb{Z}$ . Let the Galois extension of  $\mathbb{F}$  of degree  $n$  be denoted by  $\mathbb{K}$  whose ring of integers is denoted by  $\mathcal{O}_{\mathbb{K}}$  and  $Gal(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ . It is well-known that for any  $a$  in  $\mathbb{K}$ , if

$\sigma_i(a) = a \forall i = 1, \dots, n$ , then  $a \in \mathbb{F}$ . Let  $\{\theta_1, \theta_2, \dots, \theta_n\}$  be the  $\mathcal{O}_{\mathbb{F}}$ -basis of  $\mathcal{O}_{\mathbb{K}}$ .

*Trace of an element:* The trace of an element  $a \in \mathbb{K}$  in  $\mathbb{K}/\mathbb{F}$ , denoted by  $T_{\mathbb{K}/\mathbb{F}}(a)$ , is  $\sum_{i=1}^n \sigma_i(a)$  and belongs to  $\mathbb{F}$ .

*Norm of an element:* The norm of an element  $a \in \mathbb{K}$  in  $\mathbb{K}/\mathbb{F}$ , denoted by  $N_{\mathbb{K}/\mathbb{F}}(a)$ , is  $\prod_{i=1}^n \sigma_i(a)$  and belongs to  $\mathbb{F}$ .

*Discriminant of a basis* [16, p. 25]: For a chosen  $\mathbb{F}$ -basis  $\{b_1, b_2, \dots, b_n\}$ , its discriminant, denoted by  $\Delta(b_1, b_2, \dots, b_n)$ , is the determinant of the  $n \times n$  matrix  $\mathbf{M}$  whose  $(i, j)^{th}$  entry is  $T_{\mathbb{K}/\mathbb{F}}(b_i b_j)$ .

*Discriminant of  $\mathbb{K}/\mathbb{F}$*  [16, p. 148]: The discriminant of  $\mathbb{K}/\mathbb{F}$  is the ideal  $\Delta(\theta_1, \theta_2, \dots, \theta_n)\mathcal{O}_{\mathbb{F}}$ .

*Prime ideal:* An ideal  $\mathfrak{p}$  of a ring  $\mathcal{R}$  is a prime ideal if it has the following properties.

- If  $a, b \in \mathcal{R}$  such that  $ab \in \mathfrak{p}$ , then either  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ .
- $\mathfrak{p}$  is not  $\mathcal{R}$  itself.

A nonzero principal ideal is prime if and only if it is generated by a prime element.

*Prime elements of  $\mathbb{Z}[i]$ :* A Gaussian integer  $a + ib$ ,  $a, b \in \mathbb{Z}$  is a Gaussian prime if and only if either

- one of  $a, b$  is zero and the other is a prime number of the form  $\pm(4n + 3)$ , with  $n$  a nonnegative integer, or
- both  $a$  and  $b$  are nonzero and  $a^2 + b^2$  is a prime number (which will not be of the form  $4n + 3$ ).

*Prime elements of  $\mathbb{Z}[\omega]$ :* An Eisenstein integer  $z = a + \omega b$ ,  $a, b \in \mathbb{Z}$  is an Eisenstein prime if and only if either

- either  $a$  or  $b$  is zero and  $z$  is equal to the product of a unit and a natural prime of the form  $3n - 1$ , or
- both  $a$  and  $b$  are nonzero and  $|z|^2 = a^2 - ab + b^2$  is a natural prime (which is necessarily congruent to 0 or 1 modulo 3).

*Relative prime ideals:* Ideals  $A$  and  $B$  of a ring  $\mathcal{R}$  are said to be relatively prime (coprime) if  $A + B = \mathcal{R}$ . It follows that coprime ideals  $A$  and  $B$  of  $\mathcal{R}$  satisfy  $AB = A \cap B$ .

*Dedekind domain:* An integral domain  $\mathcal{R}$  which is not a field is called a Dedekind domain if every nonzero proper ideal factors into prime ideals. The ring of integers of a number field is a Dedekind domain.

*Ideal factorization in extensions* [16, p. 144]: Let  $\mathfrak{p}$  be a nonzero prime ideal in  $\mathcal{O}_{\mathbb{F}}$ . Then, in the extension field  $\mathbb{K}$  (not necessarily a Galois extension),

$$\mathfrak{p}\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^g \mathfrak{B}_i^{e(\mathfrak{B}_i/\mathfrak{p})}$$

where  $\mathfrak{B}_i \subset \mathcal{O}_{\mathbb{K}}$  are prime ideals (finite in number) in  $\mathcal{O}_{\mathbb{K}}$ ,  $e(\mathfrak{B}_i/\mathfrak{p})$  is a non-negative integer called the *ramification index* of  $\mathfrak{B}_i$  over  $\mathfrak{p}$  and is the exact power of  $\mathfrak{B}_i$  that divides  $\mathfrak{p}\mathcal{O}_{\mathbb{K}}$ .  $\mathfrak{B}_i$  is said to lie above  $\mathfrak{p}$  in  $\mathcal{O}_{\mathbb{K}}$ . This factorization is *unique* up to order of the factors since  $\mathcal{O}_{\mathbb{K}}$  is a Dedekind domain.

*Inertia degree or residue class degree* [16, p. 105]: Let  $\mathfrak{p}$  be a prime ideal in  $\mathcal{O}_{\mathbb{F}}$  that factors into prime ideals in  $\mathcal{O}_{\mathbb{K}}$  as  $\mathfrak{p}\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^g \mathfrak{B}_i^{e(\mathfrak{B}_i/\mathfrak{p})}$ . Then, the inertia degree  $f(\mathfrak{B}_i/\mathfrak{p})$  of  $\mathfrak{B}_i$  over  $\mathfrak{p}$  is a non-negative integer given by

$$f(\mathfrak{B}_i/\mathfrak{p}) = [\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i : \mathcal{O}_{\mathbb{F}}/\mathfrak{p}].$$

It follows that [16, p. 144]

$$[\mathbb{K} : \mathbb{F}] = \sum_{i=1}^g e(\mathfrak{B}_i/\mathfrak{p}) f(\mathfrak{B}_i/\mathfrak{p}).$$

*Corollary 1:* [17, p. 191] Consider a tower of field extensions  $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$  with the ring of integers  $\mathcal{O}_{\mathbb{F}} \subset \mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$ . Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_{\mathbb{F}}$ ,  $\mathfrak{B}_{\mathbb{K}}$  a prime ideal of  $\mathcal{O}_{\mathbb{K}}$  lying above  $\mathfrak{p}$  and  $\mathfrak{B}_{\mathbb{L}}$  a prime ideal of  $\mathcal{O}_{\mathbb{L}}$  lying above  $\mathfrak{B}_{\mathbb{K}}$ . Then, the ramification index and inertia degree are multiplicative in the tower, i.e.,

$$\begin{aligned} e(\mathfrak{B}_{\mathbb{L}}/\mathfrak{p}) &= e(\mathfrak{B}_{\mathbb{L}}/\mathfrak{B}_{\mathbb{K}}) e(\mathfrak{B}_{\mathbb{K}}/\mathfrak{p}) \\ f(\mathfrak{B}_{\mathbb{L}}/\mathfrak{p}) &= f(\mathfrak{B}_{\mathbb{L}}/\mathfrak{B}_{\mathbb{K}}) f(\mathfrak{B}_{\mathbb{K}}/\mathfrak{p}). \end{aligned}$$

For Galois extensions  $\mathbb{K}/\mathbb{F}$ ,  $e(\mathfrak{B}_1/\mathfrak{p}) = e(\mathfrak{B}_2/\mathfrak{p}) = \dots = e(\mathfrak{B}_g/\mathfrak{p})$  and  $f(\mathfrak{B}_1/\mathfrak{p}) = f(\mathfrak{B}_2/\mathfrak{p}) = \dots = f(\mathfrak{B}_g/\mathfrak{p})$  [16, p. 152]. In such a case, we simply denote the ramification index and the inertia degree by  $e$  and  $f$ , respectively, and

$$[\mathbb{K} : \mathbb{F}] = n = efg. \quad (17)$$

*Definition:* Let  $\mathfrak{p}$  be a prime ideal in  $\mathcal{O}_{\mathbb{F}}$  that factors into prime ideals of  $\mathcal{O}_{\mathbb{K}}$  in the Galois extension field  $\mathbb{K}$  as  $\mathfrak{p}\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^g \mathfrak{B}_i^e$  with an inertia degree  $f$ . Then,

- $\mathfrak{p}$  is *ramified* in  $\mathbb{K}$  if  $e > 1$ .
- $\mathfrak{p}$  is *totally ramified* in  $\mathbb{K}$  if  $e = n$ ,  $g = 1$ ,  $f = 1$ .
- $\mathfrak{p}$  *splits* in  $\mathcal{O}_{\mathbb{K}}$  if  $g > 1$ .
- $\mathfrak{p}$  *splits completely* in  $\mathcal{O}_{\mathbb{K}}$  if  $e = 1$ ,  $g = n$ ,  $f = 1$ .
- $\mathfrak{p}$  is *inert* in  $\mathcal{O}_{\mathbb{K}}$  if  $e = 1$ ,  $g = 1$ .

*Corollary* [16, P. 148]: A prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_{\mathbb{F}}$  is ramified in  $\mathbb{K}$  if and only if it divides the discriminant of  $\mathbb{K}/\mathbb{F}$ .

Let  $\theta \in \mathcal{O}_{\mathbb{K}}$  such that  $\mathbb{K} = \mathbb{F}(\theta)$  (not necessarily a Galois extension) with the minimal polynomial of  $\theta$  being  $p(X) \in \mathcal{O}_{\mathbb{F}}[X]$ . The *conductor* of the ring  $\mathcal{O}_{\mathbb{F}}[\theta]$  is the largest ideal  $\mathfrak{f}$  of  $\mathcal{O}_{\mathbb{K}}$  that is contained in  $\mathcal{O}_{\mathbb{F}}[\theta]$ .

*Proposition 5:* [18, p. 47] Let  $p$  be a prime integer of  $\mathcal{O}_{\mathbb{F}}$  such that  $\mathfrak{p} = p\mathcal{O}_{\mathbb{F}}$  is a prime ideal of  $\mathcal{O}_{\mathbb{F}}$  and  $\mathfrak{p}\mathcal{O}_{\mathbb{K}}$  is relatively prime to the conductor of  $\mathcal{O}_{\mathbb{F}}[\theta]$ , and let  $\bar{p}(X) = \bar{p}_1(X)^{e_1} \bar{p}_2(X)^{e_2} \dots \bar{p}_g(X)^{e_g}$  be the factorization of the polynomial  $\bar{p}(X) = p(X) \bmod p$  into monic irreducibles  $\bar{p}_i(X) = p_i(X) \bmod p$  over the residue class field  $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ , with all the  $p_i(X) \in \mathcal{O}_{\mathbb{F}}(X)$  and monic. Then,  $\mathfrak{B}_i = \mathfrak{p}\mathcal{O}_{\mathbb{K}} + p_i(\theta)\mathcal{O}_{\mathbb{K}}$ ,  $i = 1, \dots, g$ , are the different prime ideals of  $\mathcal{O}_{\mathbb{K}}$  above  $\mathfrak{p}$ . The inertia degree  $f(\mathfrak{B}_i/\mathfrak{p})$  of  $\mathfrak{B}_i$  over  $\mathfrak{p}$  is the degree of  $\bar{p}_i(X)$ , and one has

$$\mathfrak{p}\mathcal{O}_{\mathbb{K}} = \mathfrak{B}_1^{e_1} \mathfrak{B}_2^{e_2} \dots \mathfrak{B}_g^{e_g}.$$

*Theorem 1:* [19, Theorem 2.47] Let  $\mathbb{F}_q$  be a finite field with  $q$  elements and characteristic  $p$ ,  $n$  a natural number such that  $p$  does not divide  $n$ . The  $n^{th}$  cyclotomic polynomial  $\Phi_n(X)$  factorizes over  $\mathbb{F}_q$  as a product of irreducible factors all of the same degree  $d$ , where  $d$  is the order of  $q \bmod n$  ( $d$  is the smallest positive integer such that  $q^d \equiv 1 \bmod n$ ).

## APPENDIX II

PROOF THAT  $(-25 + 12i)\mathbb{Z}[i]$  DOES NOT SPLIT COMPLETELY IN  $\mathbb{Z}[i, \zeta_5]$

Let  $\mathfrak{p}_{769} = (-25 + 12i)\mathbb{Z}[i]$  which is a prime ideal of  $\mathbb{Z}[i]$ . The discriminant of  $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$  is  $125\mathbb{Z}[i]$  and clearly  $\mathfrak{p}_{769}$



does not divide  $125\mathbb{Z}[i]$ . So,  $\mathfrak{p}_{769}$  is not ramified in  $\mathbb{Q}(i, \zeta_5)$ . We have the following tower of Galois field extensions.

$$\begin{aligned}\mathbb{Q} &\subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \zeta_5), \\ \mathbb{Q} &\subset \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(i, \zeta_5)\end{aligned}$$

where  $[\mathbb{Q}(i, \zeta_5) : \mathbb{Q}] = 8$ ,  $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ . The prime ideal  $769\mathbb{Z}$  splits into two prime ideals  $\mathfrak{p}_{769} = (-25 + 12i)\mathbb{Z}[i]$  and  $\mathfrak{q}_{769} = (-25 - 12i)\mathbb{Z}[i]$  in  $\mathbb{Z}[i]$ . From Corollary 1 and (17) in Appendix I,  $769\mathbb{Z}$  splits completely in  $\mathbb{Z}[i, \zeta_5]$  if and only if  $\mathfrak{p}_{769}$  and  $\mathfrak{q}_{769}$  split completely in  $\mathbb{Z}[i, \zeta_5]$ . Also,  $769\mathbb{Z}$  splits completely in  $\mathbb{Z}[i, \zeta_5]$  if and only if it splits completely in  $\mathbb{Z}[\zeta_5]$ .

So, it is sufficient to prove that the ideal  $769\mathbb{Z}$  does not split completely in  $\mathbb{Z}[\zeta_5]$ . For this purpose, we consider the minimal polynomial of  $\zeta_5$  over  $\mathbb{Q}$ , which is  $X^4 + X^3 + X^2 + X + 1$  and is also the 5<sup>th</sup> cyclotomic polynomial  $\Phi_5(X)$ . From Theorem 1 in Appendix I,  $\Phi_5(X)$  splits into only 2 irreducible monic factors over  $\mathbb{F}_{769}$ , each of degree 2. Hence, from Proposition 5, it is clear that  $769\mathbb{Z}$  does not split completely in  $\mathbb{Z}[\zeta_5]$ . This establishes that  $(-25 + 12i)\mathbb{Z}[i]$  does not split completely in  $\mathbb{Z}[i, \zeta_5]$ .

### APPENDIX III

PROOF THAT  $(3 - 8\omega)\mathbb{Z}[\omega]$  DOES NOT SPLIT COMPLETELY IN  $\mathbb{Z}[\omega, \zeta_7]$

Let  $\mathfrak{p}_{97} = (3 - 8\omega)\mathbb{Z}[\omega]$  which is a prime ideal of  $\mathbb{Z}[\omega]$ . The discriminant of  $\mathbb{Q}(\omega, \zeta_5)/\mathbb{Q}(\omega)$  is  $7^5\mathbb{Z}[\omega]$  and clearly  $\mathfrak{p}_{97}$  does not divide  $7^5\mathbb{Z}[\omega]$ . So,  $\mathfrak{p}_{97}$  is not ramified in  $\mathbb{Q}(\omega, \zeta_7)$ . We have the following Galois field extensions.

$$\begin{aligned}\mathbb{Q} &\subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\omega, \zeta_7), \\ \mathbb{Q} &\subset \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(\omega, \zeta_7)\end{aligned}$$

where  $[\mathbb{Q}(\omega, \zeta_7) : \mathbb{Q}] = 12$ ,  $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ . The prime ideal  $97\mathbb{Z}$  splits into two prime ideals  $\mathfrak{p}_{97} = (3 - 8\omega)\mathbb{Z}[\omega]$  and  $\mathfrak{q}_{97} = (3 - 8\omega^2)\mathbb{Z}[\omega]$  in  $\mathbb{Z}[\omega]$ . It is clear from the Corollary 1 and (17) in Appendix I that  $97\mathbb{Z}$  splits completely in  $\mathbb{Z}[\omega, \zeta_7]$  if and only if  $\mathfrak{p}_{97}$  and  $\mathfrak{q}_{97}$  split completely in  $\mathbb{Z}[\omega, \zeta_7]$ . Also,  $97\mathbb{Z}$  splits completely in  $\mathbb{Z}[\omega, \zeta_7]$  if and only if it splits completely in  $\mathbb{Z}[\zeta_7]$ .

So, it suffices to prove that the ideal  $97\mathbb{Z}$  does not split completely in  $\mathbb{Z}[\zeta_7]$ . For this purpose, we consider the minimal polynomial of  $\zeta_7$  over  $\mathbb{Q}$ , which is  $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$  and is also the 7<sup>th</sup> cyclotomic polynomial  $\Phi_7(X)$ . From Theorem 1 in Appendix I,  $\Phi_7(X)$  splits into only 3 irreducible monic factors, each of degree 2 over  $\mathbb{F}_{97}$ . Hence, from Proposition 5, it is clear that  $97\mathbb{Z}$  does not split completely in  $\mathbb{Z}[\zeta_7]$ . This establishes that  $(3 - 8\omega)\mathbb{Z}[\omega]$  does not split completely in  $\mathbb{Z}[\omega, \zeta_7]$ .

### REFERENCES

- [1] F. Oggier, G. Rekaya, J. C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885-3902, Sep. 2006.
- [2] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869-3884, Sep. 2006.

- [3] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect Space-Time Codes for Any Number of Antennas," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853-3868, Nov. 2007.
- [4] F. Oggier, C. Hollanti, and R. Vehkalahti, "An algebraic MISO-MISO code construction," in *Proc. Int. Conf. Signal Process. and Commun. (SPCOM 2010)*, Bangalore, India, July 2010.
- [5] B. Hassibi and B. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804-1824, July 2002.
- [6] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space time codes for high data rate wireless communication : performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744 - 765, Mar. 1998.
- [7] L. Zheng and D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.
- [8] J. C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden Code: A  $2 \times 2$  full rate space-time code with non-vanishing determinants," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432-1436, Apr. 2005.
- [9] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753-761, Mar. 2002.
- [10] N. Jacobson, *Basic Algebra II*. 2nd ed. New York: W.H. Freeman, 1985.
- [11] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, High-rate Space-Time Block Codes from Division Algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596-2616, Oct. 2003.
- [12] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto, "On the Densest MIMO Lattices From Cyclic Division Algebras," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3751-3780, Aug 2009.
- [13] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585-595, Nov. 1999.
- [14] B.M. Hochwald and S. ten Brink, "Achieving Near-Capacity on a Multiple-Antenna Channel," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 389-399, March 2003.
- [15] E. Baccarelli, "Evaluation of the Reliable Data Rates Supported by Multiple-Antenna Coded Wireless Links for QAM Transmissions," *IEEE J. Sel. Areas Commun.*, vol. 19, no. 2, pp. 295-304, Feb. 2001.
- [16] P. J. McCarthy, *Algebraic Extensions of Fields*. New York: Dover Publications, 1991.
- [17] P. Ribenboim, *Classical Theory of Algebraic Numbers*. 2nd ed. New York: Springer-Verlag, 2001.
- [18] J. Neukirch, *Algebraic Number Theory. (Grundlehren der mathematischen Wissenschaften)*, 1st ed.: Springer, 1999.
- [19] R. Lidl and H. Niederreiter, *Finite Fields*, in *Encyclopedia of Mathematics and Its Application*, 2nd ed., vol 20, Cambridge: Cambridge University Press, 1997.